UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/365,446	08/02/1999	HIROKAZU OUGI	773-005	1802

7590 08/01/2003

JOSEPH SOFER
SOFER & HAROUN LLP
317 MADISON AVENUE
SUITE 910
NEW YORK, NY 10017

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2132	7

DATE MAILED: 08/01/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/365,446	Applicant(s) OUGI ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If the period for reply specified above is the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication (35 U.S.C. § 133).
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-22 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 02 August 1999 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because "other" in the second line should be "another" or "a different". Also, the process described in the abstract encrypts a recipient's algorithm with the recipient's algorithm and sends the cryptogram to the recipient; based on the specification, the examiner believes that the abstract's process should encrypt the transmitter's algorithm (computer 100's algorithm) with the recipient's algorithm. Correction is required. See MPEP § 608.01(b).

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claims 5-16, 20, and 22 are objected to because of the following informalities: the article before "user" is "an", not "a". Appropriate correction is required.

4. Claims 6 and 7 are objected to because of the following informalities: in the fourth line, an "a" is needed in the middle of "of transmission"; in the eighth line, "the" is needed before the first recitation of "user"; in six only, the nineteenth line needs an article after "and". In claim 8, line 22 needs an "an" after "and". Claims 9, 10, 15, and 16 need "A" at their beginnings. In claim 15, "transmitted" in the second to last line does not make any grammatical sense. It has been interpreted as though it read, like claim 9, "transmitting it" (see the comment below on this language in claim 9). In claim

16, an article is needed before "transmission" in line 22. Line 18 of claim 20 says "it is notified the user of the transmission side", which is grammatically flawed; line 7 of claim 21 is similarly incorrect. Claim 22's preamble refers to "other second encryption algorithm"; the best correction would be to replace "other" with "a". Also in claim 22, phrases such as "key . . . operated on the first encryption algorithm" (in lines 12 and 16) and "signature data written in the . . . encryption keys" (line 14) are not consistent with standard grammatical patterns; keys are not "operated on" encryption algorithms; encryption keys are not "written in". Appropriate correction is required.

Double Patenting

5. Applicant is advised that should claims 5-10 be found allowable, claims 11-16 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 17 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one

skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 17 mandates that a reception side's encryption algorithm be encrypted with a transmission side's encryption algorithm and sent to the reception side. This is not taught by the specification. The examiner has treated the claim as though the claim said that the encrypted algorithm was sent to the transmission side. This interpretation is consistent with the other claims as well as the practicality of decrypting with an algorithm that is resident with the decrypting unit.

8. Claim 21 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not teach informing the reception side that communications are disabled when a common algorithm exists between the transmission and reception side. The examiner assumes that "disabled" should read "enabled".

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 3-14, 16, and 20-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claims 3 and 4 recite the limitation "said encrypted encryption algorithm". There is insufficient antecedent basis for this limitation in the claim.

12. Claims 5-8, 11-14, and 20 refer to an user of a transmission side who is subsequently referred to as the user. The claims go on to introduce an user of a reception side, who is distinct from the user. In the following clause, a generic user whose identifier, encryption algorithm and key are stored in a database is presented. There is no distinction between the user of the transmission side and the generic user. Applicant can correct this problem by referring to the user of the transmission side as such all of the time. Applicant could clarify the claims by referring to the user of the transmission side as the first user, the user of the reception side as the second user, and the generic user as a plurality of users including the first and second users.

13. Claims 5-8, 12-14 recite the limitations "the encryption algorithm operated by the user of the transmission side" and "the encryption algorithm operated by the user of the reception side" in their second clauses. There is insufficient antecedent basis for this limitation in the claim. In all cases, change the leading "the" to "an".

14. Claims 6 and 14 recite the limitation "the encryption algorithm" spanning lines 21-22 and lines 24-25 respectively. Two encryption algorithms have already been mentioned in the claim and thus it is unclear to which this recitation refers. The examiner assumes that this reference is to the algorithm operated by the transmitting side.

15. Claim 8 recites the limitation "the signature data produced corresponding to the encryption key operated by the user of the reception side" in lines 27 and 28. There is insufficient antecedent basis for this limitation in the claim. Deleting "the" would immediately overcome this rejection, although applicant could improve the clarity of the

claim by labeling this "second signature data . . ." and dubbing the signature data sent to the transmission side "first signature data . . .."

16. Claim 9 recites the limitation "the encryption algorithm operated by the user of the reception side" in lines 8-9. There is insufficient antecedent basis for this limitation in the claim. All recitations of "the" are inappropriate. Furthermore, once these errors have been corrected, the recitation of "a reception side" in line 11 should be changed to "the reception side". Also, in line 12, "an" needs to be changed to "the". In line 14, "it" is assumed to refer to the result of the encryption, by the reception side's algorithm, of the transmission side's encryption algorithm. The clarity of the claim would be improved by "the user" in line seven being expanded to "the user of the transmission side".

17. Claims 10 and 16 recite the limitation "the user" in line 13. Three users have already been mentioned in the claim and thus it is unclear to which this recitation refers. The examiner assumes that this user is the entity at the transmission side.

18. Claims 10 and 16 recite the limitation "the obtained identifier" spanning lines 15 and 16. Two identifiers have already been mentioned in the claim and thus it is unclear to which this recitation refers. The examiner assumes that "identifier" should be pluralized.

19. Claims 12 and 14 recite the limitation "the encryption key produced based on the encryption key operated by the user of the reception side" in lines 19-21 and 22-24 respectively. There is insufficient antecedent basis for this limitation in the claim. Change "the" to "an".

20. In claim 22, the first clause is unclear because it does not clearly indicate what word or words "with a user whose encryption algorithm is to be converted" modifies; is it "querying" or "described" or something else? In both cases, using a user to perform those actions seems awkward. Should this have read "user identifier"? Similarly, "with a key" is not distinctly attached to any other phrase.

21. Claim 22 recites the limitations "the first and second encryption keys" in line 14 and "the second encryption algorithm" in line 17. There is insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 102

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

23. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Davis (6058478).

Davis presents a method of updating cryptographic information, including algorithms, in remote devices. In claims 5, 6, and 8, the most succinct description of the method, an upgrade entity generates an upgrade message (claim 5), encrypts the message with the recipient's public key (claim 6), and sends the resulting cryptogram to the remote device. The remote device accesses the cryptogram, which anticipates use

of an encryption algorithm at the remote device, authenticates the contents, and performs the upgrade (claim 5). The upgrade includes deleting a previously existing algorithm and modifying that now-deleted algorithm to update the cryptographic algorithm. As the update is now the entirety of the now-stored algorithm, it is apparent that the now-stored algorithm was sent in the upgrade message.

24. Claims 20 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Spies et al. (RE38070).

From line 43 of column 15 through line 17 of column 16, Spies et al. detail the selection of an encryption algorithm for use between two entities. This process includes obtaining the identities of the originating and receiving participants, as embodied in their encryption indices. The originating entity arrives at these values internally, and hence they come from the transmission (originating) side. The sum of these indices is shown in Table 1, which reads on applicant's database. The table shows a correspondence between a participant and encryption algorithms available to that entity, thereby anticipating the second clause of claim 20. Spies et al. say that the parties are trying to agree on an encryption algorithm, and hence the determination step is anticipated. The implication that the originating party encrypts data indicates that notification is given that a suitable algorithm exists. With respect to claim 21, the originating participant selects an algorithm and hence information indicating the encryption algorithm has been transmitted to the sender, albeit internally. Reception of a decryptable message constitutes notification at the receiving participant of enabled communications.

Claim Rejections - 35 USC § 103

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. Claim 2-6, 9-12, 15-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. in view of Davis.

Spies et al. present a system for encryption algorithm negotiation. A potential sender compares a list of the algorithms supported internally with a list of those supported by the intended recipient. They do not, however, plan a course of action for when different algorithms are used at the sending and receiving sides. Davis presents a method of upgrading encryption parameters in remote entities (see for example claims 5, 6, and 8). His scheme includes an upgrade entity encrypting encryption algorithms under an algorithm operable by the recipient of the encrypted algorithm, thereby upgrading the algorithm while ensuring the security of the algorithm. He also shows, in figure 3, a communication system between two entities where a third trusted party facilitates trust between the two entities. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Davis' algorithm update system into Spies et al.'s algorithm selection system. As both Spies et al. and Davis indicate, algorithm use is restricted by the locales of both sender and receiver, and hence it is obvious that the upgrade entity of Davis would need to know the identities of both the sender and the receiver. The sender is the only entity

that can be relied upon to know both of these identities. The joint method includes either the sender or receiver getting the updated algorithm; as such, both claims 2 and 18 are rendered obvious. Claim 17 is broader than claim 18, and hence is also rendered obvious.

Davis' fifth claim teaches including signatures within the cryptogram, thus obviating claims 3 and 19. With respect to claim 4, Davis' figure 3, which shows communications flowing from the trusted entity through the sender to the receiver, renders sending the signature with the encrypted algorithm to the sender and then to the receiver obvious.

Regarding claims 5 and 11, the combination of Spies et al. and Davis has already been shown to render obvious receiving the identities of the sender and the receiver from the sender. Spies et al. show a table that reads on applicant's data base. Davis' demonstration of encrypting an algorithm with an algorithm operable by the entity that receives the encrypted algorithm meets the limitations of the last clause of claims 5 and 11.

With respect to claims 6 and 12, which place, in the cryptogram, a key that is based on the update algorithm and an original key assigned to the cryptogram's recipient, Davis talks about altering cryptographic keys in lines 18-25 of column 2. As described in lines 56-65 of column 1, key length is one possible modification. Thus it is obvious to include in the modification instructions a key that is based on an original key as well as the update algorithm. This key, in unaltered state, is stored in the table.

In regards to claims 9, 10, 15, and 16, the upgrade entity in Davis corresponds to applicant's encryption key management station. Spies et al. have also mentioned that a mutually trusted party holds the table used to select encryption algorithms (column 15, lines 57-59). Other aspects of these four claims have already been discussed. As far as they are understood, the limitations of claim 22 are met by the preceding paragraphs.

Allowable Subject Matter

27. Claims 7, 8, 13, and 14 would be allowed were it not for the 112 issues under which they are rejected.

28. The following is a statement of reasons for the indication of allowable subject matter: the claims are allowable over the prior art because they mandate that signatures based on their respective keys be sent to both the sender and the recipient. When combined with the other features of the claims, this signature dispersal renders the claims non-obvious.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Lincke et al. (6590588) ; Richards et al. (6230267) ; Yaker (6230186); Yu et al. (6182076); Carney (6181814/5781654) – claim 18/19; Diffie et al. (Re. 36946); Borza (6076167) – figure 5; Kirby et al. (5898784) – abstract; Anderson et al. (5857025) – lines 37-40 of column 2; Ross, Jr. (5812671) – figure 1 and lines 61-64 of column 1; Talbot et al. (5679984) – paragraph spanning columns 3 and 4; Elgamal et al. (5657390) – lines 4-40 of column 7 and lines 12-17 of column 20; Miura (5509072) –

abstract; Ohno (5355413) – figures 14 and 15 as well as lines 23-45 of column 8; Wilson (5185796) – abstract; and Wiedemer (5155680).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
July 24, 2003